(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-513913
(P2005-513913A)
(43)公表日　平成17年5月12日(2005.5.12)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601D	5J104
	H04L	9/00	601E	

審査請求 未請求　予備審査請求 未請求　（全 28 頁）

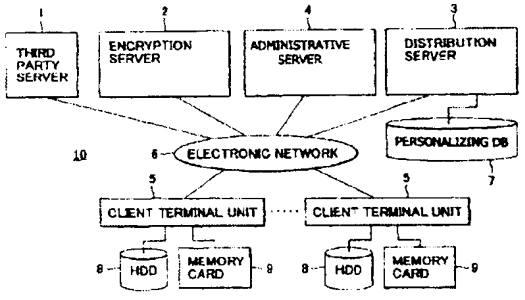
(21)出願番号　特願2003-555730 (P2003-555730)
(86)(22)出願日　平成14年12月5日 (2002.12.5)
(85)翻訳文提出日　平成16年6月11日 (2004.6.11)
(86)国際出願番号　PCT/JP2002/012738
(87)国際公開番号　WO2003/055132
(87)国際公開日　平成15年7月3日 (2003.7.3)
(31)優先権主張番号　特願2001-389452 (P2001-389452)
(32)優先日　平成13年12月21日 (2001.12.21)
(33)優先権主張国　日本国 (JP)
(81)指定国　EP (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), AU, CN, JP, KR

(71)出願人　395015319
株式会社ソニー・コンピュータエンタテインメント
東京都港区南青山二丁目６番２１号
(74)代理人　100099324
弁理士　鈴木　正剛
(74)代理人　100108604
弁理士　村松　義人
(74)代理人　100111615
弁理士　佐野　良太
(72)発明者　島田　宗毅
日本国東京都港区南青山２－６－２１　株式会社ソニー・コンピュータエンタテインメント内

最終頁に続く

(54)【発明の名称】プログラムのセキュアな配布方法及び装置

(57)【要約】
【課題】本発明に従った方法及び装置は、処理装置で暗号化されたプログラムを受信する過程と、ネットワークを通じて管理装置に機器ＩＤを伝送する過程、機器ＩＤに応答して、ネットワークを通じて登録データを受信する過程と、ネットワークを通じて登録データを配信装置に伝送する過程と、登録データに応答して処理装置でネットワークを通じて配信装置から暗号化された復号化鍵及び暗号化された仮想ＩＤを受信する過程と、仮想ＩＤを使用して暗号化された復号化鍵を復号化する過程と、及び復号化鍵を使用して暗号化されたプログラムを復号化する過程と、仮想ＩＤを使用してプログラムを再復号化する過程と、暗号化された仮想ＩＤ及び復号化プログラムを第１記録デバイスに記録する過程とを含む所定の機能の実行が可能である。



【特許請求の範囲】
【請求項１】
暗号化されたプログラムを受信するための装置であって、
ネットワークを通じて通信を行うためのネットワークインターフェースであって、（ｉ）ネットワークを通じて機器ＩＤが管理装置に送信され、（ii）前記機器ＩＤに応答して、ネットワークを通じて前記管理装置から登録データを受信し、（iii）ネットワークを通じて配信装置に前記登録データが送信され、かつ、（iv）前記登録データに応答して、前記ネットワークを通じて暗号化された復号化鍵及び暗号化された仮想ＩＤが配信装置から受信されるように前記通信を行うためのネットワークインターフェースと、
前記暗号化された復号化鍵の復号化、暗号化されたプログラムの前記復号化鍵を用いた復号化、及び前記仮想ＩＤを用いての前記プログラムの再暗号化を行うための暗号化／復号化デバイスと、
前記暗号化された仮想ＩＤと前記再暗号化されたプログラムとを記録するための第１記録デバイスと、を有する装置。
【請求項２】
前記ネットワークインターフェースは、前記機器ＩＤと配信ＩＤとを前記管理装置に前記ネットワークを通じて伝送可能で、かつ、前記機器ＩＤ及び前記配信ＩＤに応答して、ネットワークを通じて前記管理装置から前記登録データを受信するよう動作可能なものである、請求項１記載の装置。
【請求項３】
前記登録データには、少なくとも前記機器ＩＤと前記配信ＩＤとのいずれかが含まれる、請求項２記載の装置。
【請求項４】
前記機器ＩＤが前記装置に対して実質的に固有のものであり、前記仮想ＩＤが前記機器ＩＤと関連付けられている、請求項１記載の装置。
【請求項５】
前記暗号化／復号化デバイスは、前記暗号化された仮想ＩＤの前記機器ＩＤを用いた復号化、前記暗号化された復号化鍵の前記仮想ＩＤを用いた復号化、前記暗号化されたプログラムの前記復号化鍵を用いた復号化、及び前記プログラムの前記仮想ＩＤを用いた再暗号化を行うためのものである、請求項１記載の装置。
【請求項６】
前記第１記録デバイスは、更に前記機器ＩＤを記録するためのものである、請求項５記載の装置。
【請求項７】
前記暗号化／復号化デバイスは、前記暗号化された仮想ＩＤの前記機器ＩＤを用いた復号化、及び前記装置が前記プログラムを実行することが可能となるように前記再暗号化されたプログラムの前記仮想ＩＤを用いた復号化を行うためのものである、請求項６記載の装置。
【請求項８】
前記第１記録デバイスは、前記装置に対して着脱自在である、請求項６記載の装置。
【請求項９】
機器ＩＤが記録された第２記録デバイスと、
前記第１記録デバイスに記録された機器ＩＤを前記第２記録デバイスに記録された機器ＩＤと比較し、かつ、両者が一致しない場合は、前記第１記録デバイスに記録された機器ＩＤ及び前記第２記録デバイスに記録された機器ＩＤのいずれをも前記暗号化された仮想ＩＤの復号化に使用することを禁止するためのプロセッサと、を更に有する、請求項６記載の装置。
【請求項１０】
前記プロセッサは、更に、前記第１記録デバイスに記録された機器ＩＤが前記第２記録デバイスに記録された機器ＩＤと一致しない場合に、前記装置のユーザに対して、再関連

付けルーチンを選択する入力を促すように動作可能である、請求項９記載の装置。
【請求項１１】
前記ネットワークインターフェースは、更に、
前記第２記録デバイスに記録された機器ＩＤが前記第１記録デバイスに記録された機器ＩＤと一致しない場合に、前記第２記録デバイスに記録された機器ＩＤを前記ネットワークを通じて前記配信装置に伝送するよう動作可能で、かつ、
前記配信装置から前記ネットワークを通じて新たな暗号化された仮想ＩＤを受信することが可能であり、前記新たな暗号化された仮想ＩＤにおける前記仮想ＩＤは、前記第２記録デバイスに記録された機器ＩＤに関連付けられたものである、請求項９記載の装置。
【請求項１２】
前記第１記録デバイスは、更に、前記新たな暗号化された仮想ＩＤにより前記暗号化された仮想ＩＤを置換するよう動作可能なものである、請求項１１記載の装置。
【請求項１３】
前記暗号化／復号化デバイスは、前記第２記録デバイスに記録された前記機器ＩＤを用いての前記新たな暗号化された仮想ＩＤの復号化、及び前記装置が前記プログラムを実行することが可能となるように前記仮想ＩＤを用いての前記再暗号化されたプログラムの復号化を行うためのものである、請求項１２記載の装置。
【請求項１４】
前記ネットワークインターフェースは、更に、前記配信装置から前記ネットワークを通じて、前記暗号化されたプログラムを受信するためのものである、請求項１記載の装置。
【請求項１５】
前記プログラムは、アプリケーションプログラムとシステムプログラムとのいずれかである、請求項１記載の装置。
【請求項１６】
暗号化されたプログラムを処理装置で受信し、
機器ＩＤをネットワークを通じて管理装置に伝送し、
前記管理装置から、前記機器ＩＤに応答して、ネットワークを通じて前記登録データを受信し、
前記登録データを前記ネットワークを通じて配信装置に伝送し、
前記配信装置から、前記登録データに応答して、暗号化された復号化鍵と暗号化された仮想ＩＤを前記ネットワークを通じて前記処理装置で受信し、
前記暗号化された復号化鍵を前記仮想ＩＤを用いて復号化し、前記暗号化されたプログラムを前記復号化鍵を用いて復号化し、
前記プログラムを前記仮想ＩＤを用いて再暗号化し、
前記暗号化された仮想ＩＤと前記再暗号化されたプログラムとを第１記録デバイスに記録する、方法。
【請求項１７】
前記機器ＩＤと配信ＩＤとを、ネットワークを通じて前記管理装置に伝送し、
前記ネットワークを通じて、前記機器ＩＤに応答して、前記登録データを前記管理装置から受信する、請求項１６記載の方法。
【請求項１８】
前記登録データは、前記機器ＩＤ及び配信ＩＤを含む、請求項１７記載の方法。
【請求項１９】
前記仮想ＩＤが前記機器ＩＤに関連付けられる、請求項１７記載の方法。
【請求項２０】
前記暗号化された仮想ＩＤを前記機器ＩＤを用いて復号化し、前記暗号化された復号化鍵を前記仮想ＩＤを用いて復号化し、前記暗号化されたプログラムを前記復号化鍵を用いて復号化し、前記プログラムを前記仮想ＩＤを用いて再暗号化する、請求項１９記載の方法。
【請求項２１】

前記機器ＩＤと前記暗号化された仮想ＩＤとを前記第１記録デバイスに記録する、請求項２０記載の方法。

【請求項２２】

前記暗号化された仮想ＩＤを前記機器ＩＤを用いて復号化し、前記処理装置が前記プログラムを実行可能となるように、前記再暗号化されたプログラムを前記仮想ＩＤを用いて復号化する、請求項２１記載の方法。

【請求項２３】

前記第１記録デバイスは、前記処理装置に対して着脱自在である、請求項２１記載の方法。

【請求項２４】

前記処理装置は、前記機器ＩＤが記録された第２記録デバイスを有するものであり、

前記第１記録デバイスに記録された機器ＩＤを前記第２記録デバイスに記録された機器ＩＤと比較し、

これらの機器ＩＤ同士が一致しない場合は、前記第１記録デバイスに記録された機器ＩＤと前記第２記録デバイスに記録された機器ＩＤのいずれをも、前記暗号化された仮想ＩＤの復号化に使用することを禁止する、請求項２１記載の方法。

【請求項２５】

前記第１記録デバイスに記録された機器ＩＤが前記第２記録デバイスに記録された機器ＩＤと一致しない場合に、前記装置のユーザに対して、再関連付けルーチンを選択する入力を促す、請求項２４記載の方法。

【請求項２６】

前記第２記録デバイスに記録された機器ＩＤが前記第１記録デバイスに記録された機器ＩＤと一致しないときは、前記第２記録デバイスに記録された機器ＩＤを前記ネットワークを通じて前記管理装置に伝送し、

前記管理装置から新たな暗号化された仮想ＩＤを受信し、前記新たな暗号化された仮想ＩＤの前記仮想ＩＤは、前記第２記録デバイスに記録された前記機器ＩＤと関連付けられている、請求項２４記載の方法。

【請求項２７】

前記暗号化された仮想ＩＤを前記第１記録デバイスに記録された新たな仮想ＩＤで置換する、請求項２６記載の方法。

【請求項２８】

前記新たな暗号化された仮想ＩＤを前記第２記録デバイスに記録された機器ＩＤを用いて復号化し、

前記再暗号化されたプログラムを、前記処理装置が前記プログラムを実行可能となるように、前記機器ＩＤを用いて復号化する、請求項２７記載の方法。

【請求項２９】

前記暗号化されたプログラムを前記配信装置から前記ネットワークを通じて受信する、請求項１６記載の方法。

【請求項３０】

前記プログラムは、アプリケーションプログラムとシステムプログラムとのいずれかである、請求項１６記載の方法。

【請求項３１】

ネットワークを通じて通信可能なネットワークインターフェースであって、（ｉ）前記ネットワークを通じて処理装置からそれぞれの機器ＩＤが受信され、（ｉｉ）前記機器ＩＤに応答して、前記ネットワークを通じて管理装置から登録データが前記それぞれの処理装置に送信されるように前記通信を行うネットワークインターフェースと、

前記受信した機器ＩＤを記録するためのデータベースと、を備えた装置であって、

前記登録データは、暗号化された復号化鍵と暗号化された仮想ＩＤとをネットワークを通じて配信装置から入手するために前記処理装置により用いられるものであり、かつ、前記暗号化された復号化鍵は、前記仮想ＩＤを用いて前記処理装置により復号化でき、前記

暗号化されたプログラムは、前記復号化鍵を用いて前記処理装置により復号化できるものである装置。

【請求項３２】

前記ネットワークインターフェースは、更に、暗号化されたプログラムとアクティベートされていない復号化鍵とを配信装置に伝送するためのものであり、前記アクティベートされていない復号化鍵は、アクティベートされた場合は、前記暗号化されたプログラムの復号化に使用できる、請求項３１記載の装置。

【請求項３３】

前記ネットワークインターフェースは、更に（ｉ）前記ネットワークを通じて前記配信装置からアクティベート要求を受信し、かつ、（ｉｉ）前記アクティベート要求に応答して前記ネットワークを通じてアクティベート承認情報を前記配信装置に送信するためのものであり、前記アクティベート承認情報に応答して前記アクティベートされていない復号化鍵が有効化復号化鍵に変換可能である、請求項３２記載の装置。

【請求項３４】

前記ネットワークインターフェースは、更に（ｉ）実質的に固有の識別子である配信ＩＤを含む復号化鍵管理データを前記配信装置に送信し、（ｉｉ）前記配信装置から前記復号化鍵管理データ及び有効化要求を受信し、かつ、（ｉｉｉ）前記復号化鍵管理データが有効であれば、アクティベート承認情報を送信するためのものである、請求項３１記載の装置。

【請求項３５】

ネットワークを通じて処理装置からそれぞれの機器ＩＤを受信し、

前記機器ＩＤに応答して前記ネットワークを通じて登録データを前記の処理装置に送信し、

前記受信した機器ＩＤをデータベースに記録し、

前記登録データは、暗号化された復号化鍵と暗号化された仮想ＩＤとを前記ネットワークを通じて配信装置から入手するために前記処理装置で使用することができるものであり、かつ、前記暗号化された復号化鍵は、前記処理装置で前記仮想ＩＤを用いて復号化可能であり、更に、前記暗号化されたプログラムは、前記処理装置で、前記復号化鍵を用いて復号化可能である、方法。

【請求項３６】

前記ネットワークを通じて、復号化されたプログラムとアクティベートされていない復号化鍵とを配信装置に送信し、前記アクティベートされていない復号化鍵は、アクティベートされた場合は、前記暗号化されたプログラムの復号化に用いることができるものである、請求項３５記載の方法。

【請求項３７】

更に（ｉ）前記ネットワークを通じて前記配信装置からアクティベート要求を受信し、（ｉ）前記アクティベート要求に応答して前記ネットワークを通じて前記配信装置にアクティベート承認情報を伝送し、前記アクティベートされていない復号化鍵は、前記アクティベート承認情報に応答してアクティベートされた復号化鍵に変換可能である過程を含む、請求項３６記載の方法。

【請求項３８】

更に（ｉ）実質的に固有の識別子である配信ＩＤを含む復号化鍵管理データを前記配信装置に伝送し、（ｉｉ）前記復号化鍵管理データとアクティベート要求とを前記配信装置から受信し、（ｉｉｉ）前記復号化鍵管理データが有効であれば、前記アクティベート承認情報を送信する、請求項３５記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、プログラムコンテンツのセキュアな配布方法及び装置に関し、これらの方法及び装置は、上記プログラムコンテンツの不正なコピーや配布を防ぐためのものである。

【背景技術】
【０００２】
プログラムコンテンツとしては、ビデオゲームのゲームプログラム、ワードプロセッサのプログラム、表計算のプログラムや、オペレーティングシステム等のシステムプログラムやブートプログラム等が挙げられる。
コンピュータプログラム等のプログラムコンテンツは、通常、これらのプログラムコンテンツが記録されたＣＤ－ＲＯＭやＤＶＤ－ＲＯＭ等の輸送可能な記録媒体というかたちでエンドユーザに対して配布される。また、インターネットを通じてサーバからユーザがダウンロードする形態でプログラムコンテンツを配布する場合もある。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
従来のプログラムコンテンツの配布方法は、不正コピーがなされて複数のエンドユーザに行き渡ってしまうということから、セキュアなもの、つまりセキュリティ性を備えたものとはいえなかった。例えば、コンピュータプログラムプログラムが特定のエンドユーザに対して記録媒体に記録された形態で配布された場合、そのユーザが、他のエンドユーザが使用する機器に、配布されたコンピュータプログラムを不正コピーする場合が挙げられる。通常これらの不正コピーは、ハードディスク、ＣＤ－ＲＯＭ等に記録される。同様に、コンピュータプログラムがネットワークを通じてエンドユーザに配布された場合もコンピュータプログラムが不正コピーされて他のユーザに配布されるおそれがある。例えば、コンピュータプログラムが正規のエンドユーザの使用する機器に記録された後に、そのユーザがコンピュータプログラム記録媒体（例えば、光ディスク、磁気ディスク等）に記録した形態でコピーし、あるいは電子メールに添付して他のユーザにわたす場合もある。
【０００４】
従って、プログラムコンテンツのセキュアな配布を行うための新規な方法及び装置であって、プログラムコンテンツの不正コピーの増殖に関する問題を改善できるものが必要とされている。
【課題を解決するための手段】
【０００５】
本発明の一つ以上の態様によれば、暗号化されたプログラムを受信するための装置であって、ネットワークを通じて通信を行うためのネットワークインターフェースであって、（ｉ）ネットワークを通じて機器ＩＤが管理装置に送信され、（ｉｉ）前記機器ＩＤに応答して、ネットワークを通じて管理装置から登録データを受信し、（ｉｉｉ）ネットワークを通じて配信装置に前記登録データが送信され、かつ、（ｉｖ）前記登録データに応答して、前記ネットワークを通じて暗号化された復号化鍵及び暗号化された仮想ＩＤが配信装置から受信されるように前記通信を行うためのネットワークインターフェースと、前記暗号化された復号化鍵の復号化、暗号化されたプログラムの前記復号化鍵を用いた復号化、及び前記仮想ＩＤを用いての前記プログラムの再暗号化を行うための暗号化／復号化デバイスと、前記暗号化された仮想ＩＤと前記再暗号化されたプログラムとを記録するための第１記録デバイスと、を有する装置が提供される。
【０００６】
好適には、前記ネットワークインターフェースは、前記機器ＩＤと配信ＩＤとが前記管理装置に前記ネットワークを通じて伝送され、かつ、前記前記機器ＩＤ及び配信ＩＤに応答して、ネットワークを通じて前記管理装置から前記登録データを受信するためのものである。
【０００７】
好適には、前記識別情報は、実質的に機器毎に固有の機器ＩＤを含み、前記仮想ＩＤは、前記機器ＩＤと関連づけられている。好適には、前記暗号化／復号化デバイスは、前記暗号化された仮想ＩＤの前記機器ＩＤを用いた復号化、及び前記装置が前記プログラムを実行することが可能となるように前記再暗号化されたプログラムの前記仮想ＩＤを用いた

復号化を行うためのものである。前記第１記録デバイスは、更に前記機器ＩＤを記録することが可能である。

【０００８】

前記復号化装置は、前記暗号化された仮想ＩＤを前記機器ＩＤを用いて復号化することが可能であり、かつ、前記仮想ＩＤを用いて再復号化されたプログラムを実行可能とすることが望ましい。

【０００９】

前記装置は、更に機器ＩＤが記録された第２記録デバイスと、第１記録デバイスに記録された機器ＩＤと前記第２記録デバイスに記録された前記機器ＩＤとを比較し、これら機器ＩＤ同士が一致しない場合は、いずれの前記記録デバイスに記録された機器ＩＤも暗号化された仮想ＩＤの復号化のために使用を禁止することが可能であるプロセッサと、を含む。

【００１０】

前記プロセッサは、好適には、前記第１記録デバイスに記録された機器ＩＤが前記第２記録デバイスに記録された機器ＩＤと一致しない場合に、前記装置のユーザに対して、再関連付けルーチンを選択する入力を促す、あるいは入力画面を表示して上記際関連付けルーチンを選択するための入力を可能とする。前記ネットワークインタフェースは、好適に前記第２記録デバイスに記録された機器ＩＤが前記第１記録デバイスに記録された機器ＩＤと一致しない場合に、配信元である前記配信装置にネットワークを通じて前記機器ＩＤを伝送し、前記第２記録デバイスに記録された機器ＩＤと関連している新たに暗号化復号化された仮想ＩＤをネットワークを通じて前記配信装置から受信するためのものである。好適には、前記第１記録デバイスは、前記暗号化された仮想ＩＤを前記新たに暗号化された前記仮想ＩＤにより置換が可能である。前記復号化装置は、第２記録デバイスに記録された前記機器ＩＤを用いて新たに暗号化された前記仮想ＩＤを復号化し、かつ、前記装置が前記再暗号化されたプログラムの実行が可能であるような前記仮想ＩＤを用いて再暗号化されたプログラムの復号化が可能であることが好ましい。

【００１１】

本発明の更なる１つ以上の様態によれば、暗号化されたプログラムを処理装置で受信する過程と、機器ＩＤをネットワークを通じて管理装置に伝送する過程と、前記管理装置から、前記機器ＩＤに応答して、ネットワークを通じて前記登録データを受信する過程と、前記登録データを前記ネットワークを通じて配信装置に伝送する過程と、前記配信装置から、前記登録データに応答して、暗号化された復号化鍵と暗号化された仮想ＩＤを前記ネットワークを通じて前記処理装置で受信する過程と、前記暗号化された復号化鍵を前記仮想ＩＤを用いて復号化し、前記暗号化されたプログラムを前記復号化鍵を用いて復号化する過程と、前記プログラムを前記仮想ＩＤを用いて再暗号化する過程と、前記暗号化された仮想ＩＤと前記再暗号化されたプログラムを第１記録デバイスに記録する過程と、を含む方法が提供される。

【００１２】

前記方法は、更にネットワークを通じて機器ＩＤと配信ＩＤを管理装置に伝送し、及びネットワークを通じて管理装置から前記機器ＩＤと配信ＩＤに応答しての登録データを受信する過程と、を含む。

【００１３】

好適には、前記方法は、前記暗号化された仮想ＩＤを前記機器ＩＤを用いて復号化する過程と、前記暗号化された復号化鍵を前記仮想ＩＤを用いて復号化する過程と、前記暗号化されたプログラムを前記復号化鍵を用いて復号化する過程と、前記プログラムを前記仮想ＩＤを用いて再暗号化する過程と、を含む。前記方法は更に前記機器ＩＤを使用して、前記暗号化された仮想ＩＤを復号化する過程と、及び前記処理装置が前記プログラムの実行可能となるように、前記仮想ＩＤを使用して、前記再復号化されたプログラムを復号化する過程と、を含む。

【００１４】

前記方法は、好適には、第１記録デバイスに記録された機器ＩＤと第２記録デバイスに含まれる前記機器ＩＤとを比較する過程と、これら機器ＩＤが一致しない場合、前記暗号化された仮想ＩＤを復号化するためのどちらの記録デバイスにも含まれる機器ＩＤの使用を禁止する過程と、を更に含む。

【００１５】

本発明の１つ以上の形態に係る装置では、管理装置から暗号化されたプログラム及びアクティベートされていない復号化鍵とを受信可能である入力インタフェースを有し、前記アクティベートされていない復号化鍵は、アクティベートされた場合、暗号化されたプログラムを復号化するために使用可能であり、入力インターフェースを有し、この入力インターフェースは、（ｉ）ネットワークを通じて管理装置にアクティベート要求を伝送し、（ｉｉ）ネットワークを通じて管理装置から前記有効化要求に応答してのアクティベート承認情報を受信可能であるような通信を行うためのものであり、データプロセッサを有し、このデータプロセッサは、前記アクティベート承認情報に応答して前記アクティベートされていない復号化鍵をアクティベートされた復号化鍵に変換するものであり、更に、データベースを有し、このデータベースは、複数の復号化プログラムに対応するそれぞれの復号化鍵を記録するものである。

【００１６】

好適には、前記入力インタフェースは、更に（ｉ）実質的に固有の識別子である配信ＩＤを含む復号化鍵管理データを管理装置から受信し、（ｉ）前記復号化鍵管理データ及びアクティベート要求を管理装置に伝送し、及び（ｉｉｉ）前記復号化鍵管理データが有効であれば、前記アクティベート承認情報を受信するよう動作可能である。前記アクティベートされていない復号化鍵は、元々暗号化された復号化鍵であり、前記データプロセッサは、前記アクティベート承認情報を使用して、前記暗号化された復号化鍵を復号するよう動作可能である。

【００１７】

前記ネットワークインタフェースは、それぞれの処理装置に関連する登録データがネットワークを通じて処理装置から受信されるよう動作可能である。前記データベースは、それぞれ処理装置の一つに関連する各機器ＩＤの記録が可能である。前記データプロセッサは、更に、前記データベースから、受信した登録データのいずれかに一致する機器ＩＤを索出するよう動作可能であり、前記ネットワークインタフェースは、更に、前記受信した登録データに応答して、ネットワークを通じて、暗号化されたアクティベートされた復号化鍵を前記処理装置に伝送するよう動作可能であり、前記アクティベートされた復号化鍵は処理装置に施されている暗号化プログラムを復号化するために使用可能である。

【００１８】

前記登録データは、対応する処理装置に対して実質的に固有の機器ＩＤを含み、前記データプロセッサは、前記機器ＩＤに応答して、暗号化されたアクティベートされた復号化鍵を生成するよう動作可能である。好適には、前記データプロセッサは、仮想ＩＤを、前記機器ＩＤの関数として前記機器ＩＤと関連付けられるように生成し、前記アクティベートされた復号化鍵を前記仮想ＩＤを用いて暗号化し、かつ、前記仮想ＩＤを前記機器ＩＤを用いて暗号化するよう動作可能である。前記ネットワークインタフェースは、前記暗号化された仮想ＩＤを、前記ネットワークを通じて前記処理装置に対して伝送するよう動作可能である。

【００１９】

本発明のさらなる１つ以上の形態に係る装置は、（ｉ）ネットワークを通じて処理装置からそれぞれの機器ＩＤを受信し、（ｉｉ）前記機器ＩＤに応答して登録データがネットワークを通じてそれぞれの処理装置に伝送されるようにネットワークとの通信を行うネットワークインタフェースと、前記受信した機器ＩＤを記録するデータベースと、を有する。前記登録データは、前記処理装置によって、暗号化された復号化鍵及び暗号化された仮想ＩＤをネットワークを通じて配信装置から得るために使用されるものであり、前記暗号化された復号化鍵は、前記仮想ＩＤを用いて前記処理装置によって復号化可能なものであり

、前記暗号化されたプログラムは、前記復号化鍵を持って前記処理装置によって復号化可能なものである。

本発明の１つ以上のさらなる形態によると、上記装置により実行される１つ以上の動作を実現するための１つ以上の方法が考えられる。

本発明のさらなる様態、機能、効果等は、以下の説明及び添付図面等を参照すれば、この技術分野の当業者には明らかになる。

また、本発明を図示するために、現段階で好適な形態で図面を示すが、本発明は図示される手段や配置に限定されるものではないことを理解されたい。

【発明を実施するための最良の形態】

【００２０】

図１に、プログラムコンテンツを複数のエンドユーザに対して、セキュアに配布すること、例えば、プログラムコンテンツの不正なコピーが防止されるか、あるいは使用不能な状態とされるように配布することが可能なシステム１０を示す。なお、図中において、同じ要素には同じ番号を付して説明した。このシステム１０においては、好ましくは、サードパーティサーバ１と、暗号化サーバ２と、配信サーバ３と、管理サーバ４及び複数のクライアント端末５と、を含み、これらは、例えばインターネット６を通じて接続されている。なお、システム１０において、本発明の範囲を逸脱することなく、サードパーティサーバ１、暗号化サーバ２、配信サーバ４及び／又は管理サーバ４を複数設けることもできる。以下、簡素化のために、各サーバをそれぞれ一台のみ示して説明する。

各サーバ１，２，３，４は、好適には、個人やエンティティ（entity:装置、会社、団体、法人、あるいはその他の組織等であり、以下、単に「組織」と記載する）による維持や操作、及び／又は個人や組織に対してその他の関連づけがなされている。なお、サーバおよびそのサーバに関連付けられた組織に対する参照符号は、相互に入れ替えてもよい。

【００２１】

サードパーティサーバ１は、好適には、操作、維持、及び／又はその他の関連づけが、例えばプログラムコンテンツのディベロッパーと関連づけられた組織に対してなされている。一例として、サードパーティサーバ１は、コンピュータアプリケーションプログラム、コンピュータシステムプログラム等のディベロッパーとしてもよい。好適にはサードパーティサーバ１は、本発明の範囲から逸脱することなく、他の組織と関連付けられる、サードパーティサーバ１は、サーバに関連する機能を実行するための公知の（又はこれから開発される）ハードウェアを用いて構築することが可能である。

【００２２】

暗号化サーバ２は、好適には、維持、操作、及び／又は管理機能を実行できる組織に関連付けられている（その詳細は後述する）。好適にはこの組織は、前記管理サーバ４と同じ組織である。しかしながら、前記暗号化サーバ２は、本発明の範囲を逸脱することなく、他の組織と関連付けられる。前記暗号化サーバ２はサーバに関連する機能を実行するための公知（又はこれから開発される）のハードウェアのいずれを用いて構築してもよい。

【００２３】

配信サーバ３は、好適には、ネットワーク６の方法のようにクライアント端末５に前記プログラムを伝送することを実行できる組織によりコントロール、維持、及び／又は関連付けがなされる。しかしながら、前記プログラムは、記録メディアのような他のメディアを通じて伝送するようにしてもよい。前記配信サーバ３は好適に後に詳細が記載されるパーソナライジングデータベース７に接続される。前記配信サーバ３及びパーソナライジングデータベース７は、ネットワークサーバ関連機能を実行するために適用されるいずれの公知の（又はこれから開発される）ハードウェアをも使用して構築してもよい。

【００２４】

管理サーバ４は、好適には、所定の管理機能を実行することができる組織により維持、コントロール、及び／又は関連付けがなされる（その詳細は後述する）。管理サーバ４はネットワークサーバ機能及びデータベース機能を実行するために適用される、公知の（又はこれ以後開発された）ハードウェアのいずれを使用して構築してもよい。

【００２５】
以下の記載から明らかであるように、サードパーティサーバ１、暗号化サーバ２、配信装置としての配信装置サーバ３及び管理サーバ４により実行されるそれぞれの機能は、それらサーバを操作または維持し、及び／またはその他関連付けがなされた１つ以上のサーバ間及び／又は１つ以上の組織に割り当てることができる。実際、それぞれのサーバに対して個別に組織を割り当てることが要求されるわけではなく、例えば、１つの組織が暗号化サーバ３と管理サーバ４に関連付けされてもよい。しかし、上述の機能の分配は、好適には図１に示すものと一致するようになされる。

【００２６】
概略的には、それぞれのクライアント端末５は、好適にはハードディスクドライブ８、及びソニーメモリスティックのようなメモリカード９等の、公知のいずれのハードディスクドライブウェアにも動作可能であるように接続される。ハードディスクドライブ８とメモリカード９（好適にはクライアント端末５に着脱自在であるように接続される）は、装置５では別個のアイテムとして示されているが、それらは本発明の趣旨及び範囲から逸脱することなしに両者を一体のものとして装置５に配置してもよい。クライアント端末５は、パーソナルコンピュータ、ソニープレイステーション２等の公知のハードウェアのいずれを使用して構築してもよい。

【００２７】
本発明の１つ以上の形態によれば、クライアント端末５は、好適にはＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、電子メモリのような記録メディアを通じて、又はネットワーク６を通じてプログラムをダウンロードすることにより、コンピュータアプリケーションプログラムのような暗号ソースコンピュータプログラムの受信が可能である。暗号ソースコンピュータプログラムは、本発明の趣旨及び範囲から逸脱することなく、正規の会社のいずれからも入手することができるが、好適には、クライアント端末５は、暗号ソースプログラムを配信サーバ３から（ネットワーク６を通じてダウンロードすることにより）、又は、ソフトウェアディベロッパ及び／又は配信サーバ３と直接的及び／又は間接的に関連する従来の実店舗型の配信元から受信する。クライアント端末５は、またソース暗号ソースコンピュータプログラムを特定の組織から受信することは要求されず、実際、管理サーバ４，サードサーバ１又は他の組織から受信してもよい。

【００２８】
本実施形態の利点としては、エンドユーザは、クライアント端末５で最初に復号化鍵を入手して暗号ソースコンピュータプログラムを復号化しなければプログラムを実行できない形式（ソース暗号化）で、コンピュータプログラムを受信するということが挙げられる。更に、暗号化されたコンピュータプログラムが、認可されたコピーを通じて入手された場合、不正利用をしようとするエンドユーザは、最初に復号化鍵を入手しなければプログラムを実行できないであろう。下記に詳細を記載するように復号化鍵は認可されたクライアント端末５のみにより入手可能である。

【００２９】
図２に、暗号化サーバ２及びサードパーティサーバ１により実行される所定の処理ステップを示す概念的ブロック図とフロー図を示す。この図により、暗号ソースコンピュータプログラムがどのように生成されるかの一例が示される。この例において、サードパーティサーバ１は、ソフトウェアディベロッパに関連付けられており、このソフトウェアディベロッパ自体又は関連する他の組織が、コンピュータシステムプログラム、コンピュータアプリケーションプログラム等のようなプログラムを入手する。図２に示すようにサードパーティサーバ１は少なくとも１つのシステムプログラム及び少なくとも１つのアプリケーションプログラムを有する。これら１つ以上のプログラムは暗号化サーバ２にネットワークを通じて伝送される。しかし、プログラムは、例えば記録メディアを通じて暗号化サーバ２に手動で提供される。

【００３０】
暗号化サーバ２は好適にプログラムを復号化し、暗号化されたプログラムをサードパー

ティサーバ１に返信する。暗号処理は、暗号化されたプログラムを生成するために公開鍵暗号化、共通鍵暗号化等のようないずれの公知の暗号技術を採用してもよい。この例では、暗号化サーバ２は、暗号化されたシステムプログラム（ソース暗号化プログラム）及び暗号化されたアプリケーションプログラム（暗号ソースアプリケーションプログラム）をサードパーティサーバ１に返信する。本発明の実施に必須ではないが、暗号化サーバ２は暗号化されたプログラムを復号化することが可能な復号化鍵をサードパーティサーバ１に提供するようにしてもよい。好適には、復号化鍵は、アクティベートされていない状態で、つまり暗号ソースプログラムを容易に復号化できないようにして配信サーバ３に提供される。例えば、復号化鍵は、最初に、例えば暗号化サーバ２により、アクティベートされていない状態となるように暗号化される。このことにより、以下に記載するようにセキュリティのレベルを向上される。

【００３１】

以下記載するようにサードパーティサーバ１は、暗号化されたプログラムを配信サーバ３に対して記録メディアを通じて手動により配布するか、あるいはネットワーク６を通じて電子的にダウンロードすることで配布する。暗号ソースプログラムがどのように配布されるかに係わらず、エンドユーザは、好適には、以下に記載するように所定の登録手段を実施しなければプログラムを実行できないようになっている。

【００３２】

配信サーバ３と管理サーバ４で好適に実行される処理ステップを表す概念的ブロック図及びフロー図を図３に示す。配信サーバ３は好適にネットワーク６を通じて管理サーバ４と通信リンクを構築する。管理サーバ４は、好適にネットワーク６を通じて鍵配信プログラム１１、鍵管理データ１２及び鍵登録プログラム１３を配信サーバ３に伝送する。後述するように、鍵配信プログラム１１は、エンドユーザに対する復号化鍵の配信を許可するために配信サーバ３を通じて実行される。鍵管理データは、好適に情報のセキュアな集合であり、実質的に個々の配信サーバ３に固有である配信ＩＤを含む。以下でより詳細に記載するが、鍵登録プログラム１３は、非アクティブな復号化鍵をアクティブな復号化鍵（つまり暗号ソースコンピュータプログラムの復号化に使用可能である）に変換するために配信サーバ３により好適に実行される。

【００３３】

図４に、配信サーバ３と管理サーバ４との間で好適に実行される更なる処理ステップを示すフローチャートを示す。概略的には、配信サーバ３はネットワーク６を通じて管理サーバ４にアクティベート要求を実行し、これに応答して管理サーバ４からアクティベート承認情報を受信する。より詳細には、ステップＳ１において配信サーバ３は、好適にネットワーク６を通じて管理サーバ４と通信の接続をする。ステップＳ２において、配信サーバ３は、管理サーバ４に鍵管理データ（配信ＩＤを含む）を伝送する。

【００３４】

ステップＳ３において管理サーバ４は、適切な認証処理プロセスを使用して配信サーバ３を好適に認証する。例えば、管理サーバ４は、配信サーバ３が認証許可を提供するためのユーザＩＤ、パスワード等、又は他の認証可能な情報の提供の要求をするようにしてもよい。しかしながら、好適には、管理サーバ４は配信サーバ３を認証するために、鍵管理データ１２から配信ＩＤを抽出する。ステップＳ４において、認証が成功したかどうかが判定される。認証が成功しなかった場合、ステップＳ５への処理に進み、アクティベートは許可されず、処理も終了する。認証が成功した場合、好適にＳ６の処理へと進み、ここではアクティベート承認情報が管理サーバ４からネットワーク６を通じて配信サーバ３に伝送される。

【００３５】

ステップＳ７において、配信サーバ３は好適に暗号ソースコンピュータプログラムに関連した復号化鍵をアクティベートする。より詳細には、配信サーバ３はアクティベート承認情報を入力として要求する鍵登録プログラム１３を好適に実行する。これに応答して鍵登録プログラム１３は、暗号ソースコンピュータプログラムの復号化に使用できるように

復号化鍵を有効化する。一例として、アクティベート承認情報には、予め暗号化された復号化鍵の復号化に適用できる復号化鍵を有する。この場合、鍵登録プログラム１３は、予め暗号化された復号化鍵をアクティベート承認情報を用いて復号化が可能なものとなっている。

【００３６】

復号化鍵がどのようにアクティベートされたか、また、アクティベートがなされたか否かにかかわらず、配信サーバ３は、好適にパーソナライジングデータベース７内に復号化鍵を記録する。この段階において、配信サーバ３は、暗号ソースコンピュータプログラムとそのようなプログラムの復号化が可能な復号化鍵とを有すること（もしくはこれらにアクセスできる状態）となる。

【００３７】

暗号ソースコンピュータプログラムの処理のために好適に実行される所定のステップを示す概念的ブロック及びフローの説明図を図５に示す。図５に示すように、クライアント端末５は、好適にネットワーク６を通じてのダウンロード又はＣＤ－ＲＯＭ１０のような記録媒体を通じて暗号ソースコンピュータプログラムを受信済みである。クライアント端末５は、配信サーバ３から暗号ソースコンピュータプログラムを入手済みであるすることが好ましい。しかしながら、暗号ソースコンピュータプログラムを実行するためには、クライアント端末５は所定の登録ステップを実行しなくてはならない。これらのステップは、好適にネットワーク６を通じて管理サーバ４を示して説明される。

【００３８】

図６のフローチャートに、登録プロセスの一部を示す。ステップＳ２０において、クライアント端末５は上記したように暗号ソースコンピュータプログラムを受信して後述するように記録する。ステップＳ２２において、ユーザは、コンピュータプログラムをインストールして使用可能状態とする意思を示す命令を好適に入力する。これに関してクライアント端末５は、好適には、ユーザのインストール指示に応答して起動するプログラムを有する。このプログラムは、ユーザに暗号化コンピュータプログラムの登録の入力を受け付ける状態となること等によって登録を促し、通信機能を起動させる（ステップＳ２４）。

【００３９】

クライアント端末５は、好適には、ネットワーク６を通じて技術分野において公知の通信可能なネットワークインタフェイスを有する。実際、この目的のために公知のいずれのネットワークインタフェイスハードウェアを採用してもよい。ステップＳ２６において好適にクライアント端末５により通信経路形成が開始され、端末５と管理サーバ４間に当該通信経路が確立される。クライアント端末５のネットワークインタフェイスは、好適にネットワーク６を通じて端末５に関連付けられた少なくとも何らかの識別情報を管理サーバ４に送信することを容易に可能にする。詳細には、識別情報は、好適には実質的にクライアント端末５に固有である機器ＩＤを含む。識別情報は、暗号ソースプログラムの入手元（配信サーバ３）を示す配信ＩＤを含むものとしてもよい。

【００４０】

好適には、クライアント端末５は、暗号ソースプログラム及び後述する所定の他の情報を記録可能であるハードディスクドライブ８、メモリカード９等の第１記録デバイスと、機器ＩＤの記録が可能であるＲＯＭのような第２記録デバイスと、を含む。好適には、クライアント端末５のネットワークインターフェースは、更に、ネットワーク６を通じて機器ＩＤを（ＲＯＭから）管理サーバ４に伝送可能なものとなっている（動作ステップＳ２８）。

【００４１】

動作ステップＳ３０において、管理サーバ４は、好適には登録データを再生してネットワーク６を通じてクライアント端末５に伝送する。例として登録データは、機器ＩＤ及び配信ＩＤにより構築され、好適には、これらのＩＤは、その後の登録データの適切な分析により識別される。登録データを受信すると、クライアント端末は、好適にハードディスクドライブ及び／又はメモリカード９のような第１記録デバイスに同データを記録する。

【００４２】
図７において、管理サーバ４は、データベース７Ａに接続できることが示される。データベース７Ａは、上記登録処理段階で受信されたデバイスＩＤ及び／又は配信ＩＤも含むようにしてもよい。好適には、デバイスＩＤ及び配信ＩＤは、有用な履歴データ及び分析が入手されるように互いに関連付けられて記録される。例えば、上述の分析から、あるクライアント端末５が、ある配信サーバ３から暗号ソースコンピュータプログラムを受信済みの状態になったと判定することもできる。配信サーバ３から入手したデータに関連して（以下更に記載する）、デバイスＩＤ、配信ＩＤ及び／又はこれらＩＤ間の関連付けは、配信サーバ３側における義務条項（例えば契約による）がすべて満たされていることを保証するように用いることもできる。

【００４３】
図８と図９は、それぞれコンピュータプログラムを登録してエンドユーザによる実行を可能とするために好適に実行される更なる処理ステップを示す概念ブロック図及びフローチャートである。ユーザは、好適には、暗号ソースコンピュータプログラムを復号化するために適切な復号化鍵を入手するという意志表示をクライアント端末５に対して行う。ステップＳ２１において、クライアント端末５は、ネットワーク６を通じて配信サーバ３と通信リンクを確立する。その後、クライアント端末５は、配信サーバ３に（予め管理サーバ４から入手された）登録データを伝送する（動作ステップＳ２２）。

【００４４】
動作ステップＳ２３において、配信サーバ３は、ネットワーク６を通じてクライアント端末５から例えば機器ＩＤを含む（配信元ＩＤを含んでいてもよい）登録データを受信する。これに関して、配信サーバ３は、好適にはネットワーク６を通じてクライアント端末５から登録データを受信できるように通信を行うためのネットワークインタフェイスを含む。ステップＳ２３において、管理サーバ４は、また、他のＩＤ、ここでは仮想ＩＤと呼ぶＩＤを割り当て、この仮想ＩＤは、好適には、クライアント端末５から受信した機器ＩＤに対応する。仮想ＩＤは、既存の複数のＩＤから選択してもよく、また、機器ＩＤ、配信ＩＤ及び又はその他の演算対象に対する数値演算で得るようにしてもよく、あるいは、その他公知のあるいはこれから開発される技術を用いて仮想ＩＤを生成してもよい。

【００４５】
配信サーバ３は、パーソナライジングデータベース７から、クライアント端末５から受信した機器ＩＤ（つまり第２記録デバイス（ＲＯＭ）に記録された機器ＩＤ）に一致する既存の機器ＩＤを索出する。図１０を参照するとパーソナライジングデータベース７は、好適には、それぞれのクライアント端末５に対応するそれぞれの機器ＩＤの記録が可能である。図１０の左欄に示すようにパーソナライジングデータベース７には複数の機器ＩＤが予め記録されている。これら個々の機器ＩＤは、クライアント端末５のうちの１つと関連付けられ、そしてそのような機器ＩＤは、実質的にそれぞれのクライアント端末５に対して固有であることが好ましい。好適には、配信サーバ３もネットワーク６を通じてクライアント端末５から受信した機器ＩＤに一致する登録情報（例えば機器ＩＤ）に関するパーソナライジングデータベース７を検出できるデータプロセッサを好適に含む。公知の又はこれから開発されるデータプロセッサハードウェアのいずれをもこの目的のために採用してよい。

【００４６】
再度図９を参照すると、ステップＳ２３では、仮想ＩＤは、パーソナライジングデータベース７に記録された機器ＩＤに関連付けられている。つまり、受信した機器ＩＤを配信サーバ３に伝送する特定のクライアント端末５に対して、仮想ＩＤが関連付けられている。この関連付けは、記録された機器ＩＤに対応するように仮想ＩＤをパーソナライジングデータベース７内に記録することにより達成される。例えば、クライアント端末５から受信された機器ＩＤがＫ２３４５（図１０）であり、生成された仮想ＩＤがＢ５６７８である場合、機器ＩＤＫ２３４５と仮想ＩＤＢ５６７８の関連付けは、パーソナライジングデータベース７内における記録された機器ＩＤＫ２３４５に対応する（又はリンクされた）

位置に仮想ＩＤＢ５６７８を記録することで達成される。同様に、受信された機器ＩＤがＫ６７８９であり、かつ再生された仮想ＩＤがＢ９０１２であれば、機器ＩＤＫ６７８９と仮想ＩＤＢ９０１２の関連付けは、パーソナライジングデータベース７内の機器ＩＤＫ６７８９に関連付けられた位置に仮想ＩＤＢ９０１２を記録することで達成される。

【００４７】

機器ＩＤＫ１２３４とＫ０９８７の反対の位置にある仮想ＩＤ内の“--”は、関連するクライアント端末５がエンドユーザによりまだ購入されていないか、又はそのようなエンドユーザが、配信サーバ３によるコンピュータプログラムの登録をまだ行っていないことを示す。

【００４８】

上記したように、クライアント端末５からネットワーク６を通じて配信サーバ３に伝送された（ステップＳ２２，図９）登録データは、暗号ソースプログラムが入手される配信サーバ３に対応する配信ＩＤを含んでも良い。本発明の他の実施形態では、登録データ内に含まれる配信ＩＤは、機器ＩＤと関連付けられてパーソナライジングデータベース７にも記録される。

【００４９】

図９に示されるように、配信サーバ３は、好適には、暗号化された復号化鍵及び暗号化された仮想ＩＤを生成するよう動作可能であり、ここで、復号化鍵はクライアント端末５で暗号ソースコンピュータプログラムを復号化するために用いられるものである。配信サーバ３は、暗号化サーバ２（図１～図２）により生成されたそれぞれの暗号ソースコンピュータプログラムを復号化するために使用される復号化鍵がいくつであっても、これらの復号化鍵にアクセスできるようにしてもよい。これら復号化鍵は暗号化サーバ２及び／又は他の適切な組織を通じて配信サーバ３に提供される。更に、これらの復号化鍵は、ネットワーク６及び他のネットワークを通じて、又は記録メディア等を通じて手動で配信サーバ３に提供される。

【００５０】

ステップＳ２４において、配信サーバ３は、好適には、クライアント端末５と関連する仮想ＩＤを使用して復号化鍵を暗号化する。更に、配信サーバ３は、仮想ＩＤを、クライアント端末５の関連付けられた機器ＩＤを使用して暗号化する。これらの仮想ＩＤ及び機器IDは、好適には、パーソナライジングデータベース７からそれぞれが入手される。

【００５１】

配信サーバ３のネットワークインタフェースは、好適には、ネットワーク６を通じて、暗号化された復号化鍵、及び暗号化された仮想ＩＤの伝送（ステップＳ２５）をクライアント端末５に伝送するためのものとなっている。ステップＳ２６では、クライアント端末５は、好適には、暗号化された復号化鍵及び暗号化された仮想ＩＤをネットワークを通じて受信し、そして第１記録デバイス（ハードディスクドライブ８、メモリカード９等）に記録する。動作ステップＳ２７では、配信サーバ３は、好適に特定の復号化鍵がクライアント端末５に伝送されたことを（履歴データとして）記録する。この情報は、好適には、後に例えばネットワーク６を通じて、管理サーバ４に提供される。好適には、配信サーバ３は、履歴データに含まれているデータにアクセスすることができない。このデータは、決済目的のためや、債務関係の追跡等に使用される。

【００５２】

本実施形態の利点としては、暗号化された復号化鍵は、正規のクライアント端末５のみに提供されるということが挙げられる。正規のクライアント端末５として、例えば、有効な機器ＩＤを有し、復号化鍵を暗号化するために使用する仮想ＩＤと関連する機器ＩＤを登録したクライアント端末５が挙げられる。更に、ネットワークの不正行為又は不正コピー等によって、暗号化された復号化鍵を傍受しても、暗号ソースコンピュータプログラムを復号化するために必要な情報（即ち、使用可能な復号化鍵）を得ることはできない。実際、そのような復号化鍵は、実質的に固有である仮想ＩＤにより暗号化される。同様に、暗号化されたその仮想ＩＤは、登録処理が完了してクライアント端末５が認可されたとみ

なされた後にのみクライアント端末機器５に提供される。仮想ＩＤが、配信サーバ３からクライアント端末５に暗号化された手法（即ち、クライアント端末５の機器ＩＤを使用する手法）で配信サーバ３から伝送されるので、暗号化された仮想ＩＤをどのように不正に入手しても、暗号化された復号化鍵を復号化するために必要な情報は得られない。

【００５３】

暗号ソースコンピュータプログラムをクライアント端末５内にロード／インストールするために実行される所定の処理を図１１と図１２に示す。図１１においては、クライアント端末５は第１記録デバイス、つまりハードディスク８、メモリカード９等とは別個のものとして示される。しかしながら、上記したようにこれらの構成要素は本発明の請求項の趣旨と範囲から逸脱することなく、一体又は半一体な状態とすることもできる。プロセスのこの段階において、クライアント端末５は、第２デバイス、例えばＲＯＭ、に記録された機器ＩＤを含み、一方、第１記録デバイス８，９には、機器ＩＤ、暗号化された仮想ＩＤ、暗号化された復号化鍵、及び暗号ソースコンピュータプログラムが記録されている。

【００５４】

ステップＳ５０（図１２参照）において、ユーザは、将来の使用のために暗号ソースコンピュータプログラムをロード／インストールするための指示をクライアント端末５に提供する。これに応答してクライアント端末５は、適切なハードウェア及びソフトウェアを使用して第１記録デバイス８，９から機器ＩＤを読み取り、第２デバイス、すなわちＲＯＭから機器ＩＤを読み取る（ステップＳ５２）。ステップＳ５４において、これらの機器ＩＤが一致するか否かが判定される。これらが一致しない場合、処理は終了し、及び／又はその他の処理に入る。しかしながら、これらが一致した場合、ステップＳ５６に進み、暗号化された仮想ＩＤを、機器ＩＤ（好適にはＲＯＭに記録された機器ＩＤ）を使用して復号化する。仮想ＩＤが入手された後に、暗号化された復号化鍵は仮想ＩＤを使用して復号化される（ステップＳ５８）。次に暗号ソースコンピュータプログラムが復号化鍵を使用して復号化される（ステップＳ６０）。ステップＳ６２では、ステップＳ５６で入手された仮想ＩＤを使用してコンピュータプログラムが再度暗号化され、クライアントで暗号化されたコンピュータプログラムが得られる。このクライアントで暗号化されたコンピュータプログラムは、第１記録デバイス８，９内に記録される（ステップ６４）。この段階では、暗号化された復号化鍵も暗号ソースコンピュータプログラムも第１記録デバイス８，９に保存される必要はない。

【００５５】

クライアント端末５は、好適には、上記したように暗号化／復号化機能を実行するために暗号化デバイス及び復号化デバイスを含む。暗号化デバイス及び復号化デバイスは、一体のものとしてもよく、簡単のため復号化デバイスと称する。このような暗号化／復号化を実行するために公知の又はこれから開発されるいずれのハードウェア及び／又はソフトウェアをも本発明に用いることができる。例えば、復号化ライブラリー、暗号化ライブラリー等を用いることができる。

【００５６】

本実施形態では、クライアント暗号化コンピュータプログラムはセキュアなものであるという利点がある。何故ならば（以下に説明されるように）他のクライアント端末５において不正なエンドユーザが不正なコピーを実行することはできないからである。実際、クライアントで暗号化されたコンピュータプログラムは、最初に復号化されなくてはならないが、以下に説明するように、このような復号化は、配信サーバ３によりコンピュータプログラムを登録されたクライアント端末５以外では実行することはできない。

【００５７】

クライアント端末５により実行されるコンピュータプログラムの処理を図１３，１４を参照して説明する。この処理段階では、クライアント端末５は、機器ＩＤが記録された第２記録デバイス、例えばＲＯＭと、機器ＩＤ、暗号化された仮想ＩＤ、クライアントで暗号化されたコンピュータプログラムとが記録された第１記録デバイス８，９と、を有する。

【００５８】
ステップＳ７０において、ユーザは、クライアント端末５にコンピュータプログラムを実行するための命令を与える。これに応答して、クライアント端末５は、適切なコンピュータプログラムの制御下で動作し、第１記録デバイス８，９から機器ＩＤを復号化し、及び第２記録デバイス（ＲＯＭ）から機器ＩＤを復号化する（ステップＳ７２）。ステップＳ７４において、これらの機器ＩＤが互いに一致するかどうか決定される。それらが一致しない場合、処理フローは、図１５～１８を参照して以下詳細を記載する再登録処理へと進む。これらの機器ＩＤが一致した場合、処理フローは、クライアント端末５の復号化デバイスが機器ＩＤ（好適にＲＯＭに含まれる）を使用して、暗号化された仮想ＩＤを復号化するステップＳ７６へ進む。ステップＳ７８では、クライアント端末５の復号化デバイスは、ステップＳ７６で入手された仮想ＩＤを使用して、クライアント暗号化コンピュータプログラムを復号化する。この時点で、クライアント端末５はＲＡＭに存在するコンピュータプログラムを実行する。

【００５９】
本実施形態の利点としては、クライアントで暗号化されたコンピュータプログラムは、クライアント暗号化コンピュータプログラムを暗号化するために使用される仮想ＩＤに関連するクライアント端末５を使用することによってのみ復号化されることが挙げられる。従って、クライアントで暗号化されたコンピュータプログラムの不正なコピーが正規ではないエンドユーザに提供された場合、その正規ではないエンドユーザがコンピュータプログラムを実行しようとしても、暗号化されたコンピュータプログラムを復号化することはできない。更に第１記録デバイス８，９が正規ではないエンドユーザ（例えば、記録媒体８，９が他のクライアント端末５に接続されている場合）に提供された場合、暗号化された仮想ＩＤは、ＲＯＭに記録されている機器ＩＤが第１記録デバイス８，９に含まれている機器ＩＤと一致しない限り復号化されない。従って、クライアントで暗号化されたコンピュータプログラムを復号化することは不可能である。コンピュータプログラムのセキュアな配信に対するこの斬新なアプローチによって、コンピュータプログラムの不正なコピーを使用不可にしたり、及び特定のクライアント端末５のみがコンピュータプログラムを実行を可能にすることが保証される。

【００６０】
上述のように、コンピュータプログラムは、コンピュータプログラムビデオゲーム、ワードプロセッサプログラム、表計算ソフト等のようなアプリケーションプログラムであり、又はオペレーティングシステム（ＯＳ）、ブートプログラム等のシステムプログラムである。

【００６１】
上記したように図１３，１４を参照すると、ユーザがクライアント暗号化コンピュータプログラムの実行の意志を示した場合、第１記録デバイス８，９に含まれる機器ＩＤとクライアント端末５の第２記録デバイス（ＲＯＭ）に含まれる機器ＩＤとが一致するかどうかがステップＳ７４で判定される。これらの機器ＩＤが一致しない場合、処理フローは図１５を参照して記載される再登録処理へと分岐する。

【００６２】
クライアント端末５が、別のクライアント端末機器５の記録デバイス８，９と接続されるという不適切な変更がなされた場合、これらの機器ＩＤは一致しない。一方、クライアント端末５が修理され、この修理に伴って第２記録デバイスＲＯＭに記録された機器ＩＤが変更された場合も、これらの機器ＩＤは互いに異なるものとなる。また更に、例えばユーザが何らかの理由でクライアント端末を新たなクライアント端末５と入れ替え、その一方で第１記録デバイス８，９には、ひとつ又は二つ以上のクライアントで暗号化されたコンピュータプログラムが記録されていることから、この第１記録デバイスをそのまま交換しなかったという場合でも、これらの機器ＩＤは一致しなくなる。いずれの場合においても、本発明によれば再登録（又は更新登録）処理がなされる。これらの機器ＩＤが互いに一致しない場合、たとえコンピュータプログラムを正規に入手していたとしても、第１記

録デバイス８，９に保存されているコンピュータプログラムを実行することはできない。当然、ユーザはコンピュータプログラムを（もとの暗号ソースの形式で容易に入手可能だとしても）再インストール可能であるが、しかしながら、本発明によれば、この相当困難な処理を回避することができる。

【００６３】

図１５の主記録デバイスの詳細を記載する前に、第１記録デバイス８，９に記録されたコンピュータプログラムやデータに対しては、前述の図面とはその名称の付け方が多少異なっていることに留意されたい。詳細には、第１記録デバイス８，９は、パーソナル化されたシステムプログラム、パーソナル化されたアプリケーションプログラム、及びパーソナライジング情報と、を含む。パーソナル化されたシステムプログラム及びパーソナル化されたアプリケーションプログラムは、上記したようにクライアントで暗号化されたプログラムと関連する。パーソナライジング情報は、機器ＩＤと、配信ＩＤと、暗号化された仮想ＩＤのうちの一つ以上に関連する。

【００６４】

図１５を更に詳細に説明すると、旧クライアント端末又は故障したクライアント端末５Ｆがサポートセンター１１に送られる処理が示され、このサポートセンター１１で修理又は交換が行われて、新たなクライアント端末装置５Ｎがユーザに提供される。好適には、サポートセンター１１は、新たなクライアント端末５Ｎから配信サーバ３に新たな機器ＩＤを伝送するのみならず、故障した端末装置５Ｆからの旧機器ＩＤをも配信サーバ３に伝送する。

【００６５】

更に図１６と図１７を参照すると、好適には、配信サーバ３は故障した端末５Ｆから旧機器ＩＤを、新たなクライアント端末５Ｎからの新たな機器ＩＤとともに受信する。その後、配信サーバ３はパーソナライジングデータベース７にアクセスし、旧クライアント端末５Ｎの機器ＩＤ、例えば機器ＩＤＫ６７８９を検出する。この検出は、関連付けられた仮想ＩＤＢ９０１２（及び媒体ＩＤＭ２４６８も）を入手するために行われる。次にパーソナライジングデータベース７に記録された機器ＩＤから、新たなクライアント端末装置５Ｎの新たな機器ＩＤＫ１１４３が索出される。次に旧機器ＩＤＫ６７８９と関連付けされた仮想ＩＤＢ９０１２が、新たな機器ＩＤＫ１１４３（及び旧媒体ＩＤにも）関連付けられる。この処理段階で、配信サーバ３は、ユーザがユーザ自身の登録情報を更新できる状態となる。

【００６６】

前述のように、ユーザが、第１記録デバイス８，９に存在するコンピュータプログラムの実行をクライアント端末装置５Ｎに命令すると、第１記録デバイス８，９及び第二記録デバイス（ＲＯＭ）に記録された各機器ＩＤが一致するかどうかが判定される（ステップＳ７０－Ｓ７４，図１４参照）。更に、図１８に示されるように、両機器ＩＤが一致しないと判定されると（ステップＳ７４，図１４参照）、ユーザに対して、好適には、配信サーバ３に対して登録情報の更新を行うことが促される（ステップＳ５１）。ステップＳ５２において、ユーザがクライアント端末５に登録更新処理実行の指示をしたかどうか判定される。そのような指示が受信されない場合、好適にはＳ５１に戻り、ユーザは再度登録情報を更新するように促される。ユーザが登録情報をアップデートするための指示を出した後に、処理は好適にはステップＳ５２からステップＳ５３へと進み、新たなクライアント端末装置５Ｎの第２記録デバイス（ＲＯＭ）に含まれる機器ＩＤがネットワーク６を通じて配信サーバ３に伝送される（ネットワークインターフェースによる）。Ｓ５４において、管理サーバは、パーソナライジングデータベース７にアクセスすることでこの情報を確認する。その後、旧仮想ＩＤ（本来旧クライアント端末５Ｆに関連付けられていた仮想ＩＤ）は新たな機器ＩＤ（Ｋ１１４３）を使用して暗号化され、ネットワーク６を通じて（例えば配信サーバ３のネットワークインタフェースを通じて）新たなクライアント端末５Ｎに伝送される。

【００６７】

ステップＳ５６において、新たなクライアント端末５Ｎは、新たな暗号化された仮想ＩＤ（パーソナライジングデータベース情報）を受信し、そして好適には、暗号化された旧仮想ＩＤを入れ替えるという手法で、第１記録デバイス８，９に記録する。これで登録アップデート処理は完了する。

【００６８】

本実施形態では、元々は故障したクライアント端末５Ｆに使用されていたクライアント暗号化コンピュータプログラムを、新たな暗号化された仮想ＩＤを用いて復号化することができるという利点が得られる。何故なら、新たな暗号化された仮想ＩＤは、旧暗号化された仮想ＩＤと同じ仮想ＩＤを含むからである。換言すると、旧暗号化された仮想ＩＤと新たに暗号化された仮想ＩＤとは、仮想ＩＤを暗号化するために使用される機器ＩＤのみが異なるに過ぎない。ユーザが新たなクライアント端末５Ｎ上でクライアント暗号化コンピュータプログラムを実行するために、図１３，図１４を参照した上記の処理ステップが実行される。

【００６９】

図１９に、本発明の他の１つ以上の実施例を示す処理フローチャートを示す。本発明のこの実施例は、レンタルプログラムの配信元からの安全なプログラムの伝送を目的とする。レンタルプログラムの配信元はサードパーティサーバ１、管理サーバ４、配信サーバ３、又は他のサーバ（示されていない）としてよい。クライアント端末５のユーザが、プログラムコンテンツのレンタルを望む場合、ユーザは、好適には、レンタルシステムの会員になることが要求される。これに関してステップＳ７０では、例えば、クライアント端末５のアクティベート機構を通じて、このレンタルシステムの会員になる意思表示を行う。例として、クライアント端末５は、入会処理を容易にする適切なコンピュータプログラムを含み、このコンピュータプログラムを実行する。

【００７０】

ステップＳ７２において、クライアント端末５は、好適にネットワーク６を通じて管理サーバ４と通信リンクを確立する。ステップＳ７４において、クライアント端末５によるレンタルシステムの会員になるという要求がなされ、好適にはクライアント端末５がネットワーク６を通じて機器ＩＤを管理サーバ４に伝送する。これに応答して管理サーバ４は、実質的にクライアント端末５に固有である電子会員証明書を生成する。管理サーバ４は、例えば本発明の上述の実施例のデータベース関連技術を使用して電子会員証明書とクライアント端末５の機器ＩＤとを関連付ける。ステップＳ８０において、管理サーバ４は、好適にネットワーク６を通じてクライアント端末５に電子会員証明書を伝送する。後述するように、電子会員証明書はレンタル処理において使用される。

【００７１】

クライアント端末５が、レンタルシステムの会員になった後、ユーザは、好適にはアプリケーションプログラム及びシステムプログラムのようなプログラムをレンタルする許可が提供される。好適な実施例では、プログラムコンテンツはビデオコンピュータプログラムである。図２０に示されるように、クライアント端末５で実行されているコンピュータソフトウェアによって、好適には、ユーザがコンピュータプログラムをレンタルする意思表示を行うことができる。このユーザからの指示に応答して（ステップＳ８２）、クライアント端末５が、配信元との間に通信リンクを確立し、この通信リンクを通じて、ユーザによるレンタル要求が配信装置に配信される。（ステップＳ８４）。ステップＳ８６において、配信装置では、例えば、クライアント端末５の機器ＩＤを分析することにより、又は電子会員証明書を解析することにより、好適にクライアント端末５を識別する。これは、クライアント端末５が、機器ＩＤ及び／又は電子会員証明書を配信装置に提供すること、及び配信装置がこの情報が認証されるデータベースへのアクセスを有すること、を要求することにより達成される。

【００７２】

クライアント端末５が識別されたと仮定して、配信装置は、好適にネットワーク６を通じてクライアント端末５にレンタル可能なタイトルのリスト又はメニュを提供する（ステ

ップＳ８８）。クライアント端末５に実行されているコンピュータソフトウェアは、ユーザがタイトルを選択し、レンタル期間を指定できるようにユーザにタイトルのリスト又はメニュを好適に表示するためのものである（ステップＳ９０）。ユーザの選択結果及び指定されたレンタル期間は、ネットワーク６を通じて配信装置へ好適に伝送される。

【００７３】

ステップＳ９２において、配信装置は、好適には、クライアント端末５が指定した期間分のコンピュータプログラムのレンタル料に相当する送金を行うことを要求する。これは、公知の技術のいずれをも使用して、例えばクレジットカード番号、需要者の預金口座番号、請求決済等を伝送することにより、達成される。送金が実行された後に、好適には配信装置は指定されたタイトルのレンタル期間に関する送金が為されたことを示す電子決済チケットを生成する（ステップＳ９４）。ステップＳ９６において、配信装置はネットワーク６を通じて好適に電子決済チケットをクライアント端末５に伝送する。

【００７４】

本発明によれば、電子決済チケットは、ユーザ（又はクライアント端末５）に対して、配信元への送金がされると、所定のレベルのレンタル権を好適にユーザに提供する。例えば、これらのレンタル権では、コンピュータプログラムのタイトル、レンタル期間、送金代価等が特定されている。加えて電子決済チケットは、コンピュータプログラムの復号化が可能である復号化鍵のように、付加情報を含むようにできる。電子決済チケットが復号化鍵を含むことは必須ではない。実際、このように復号化鍵を電子決済チケットに含めることは、単に一例に過ぎない。電子決済チケットは、例えば、復号化鍵を、暗号化された状態で含むようにしてもよい。この暗号化は、機器ＩＤを使用して暗号化することにより、又は電子会員証明書（仮想ＩＤ等）の一部の情報を使用することにより行うことができる。いずれにしても、処理のこの時点において、ユーザは、所定のレベルのレンタル権を好適に受信するが、コンピュータプログラム又は暗号化されたコンピュータプログラムまだ受信してはいない。

【００７５】

処理のこの段階でクライアント端末５は、機器ＩＤと、電子会員証明書と、あるタイトルの一定期間レンタル分の送金がなされたことを示す電子決済チケットを有する。図２１に示されるように、クライアント端末５は、ネットワーク６を通じて好適に管理サーバ４と通信リンクを構築する（ステップＳ９８）。ステップＳ１００において、管理サーバ４は、機器ＩＤ又は電子会員証明書によりクライアント端末５を識別する。これは、予め付与された電子会員証明書とクライアント端末装置５の機器ＩＤとの関連付けが記録された、パーソナライジングデータベース６のような適切なデータベースにアクセスすることにより達成される。ステップＳ１０２において、クライアント端末５は、ネットワーク６を通じて管理サーバ４に好適に電子決済チケットを送信する。これに応答して、管理サーバ４は、電子レンタルチケットを好適に生成し（ステップＳ１０４）、ネットワーク６を通じてクライアント端末５に電子レンタルチケットを伝送する（ステップＳ１０６）。

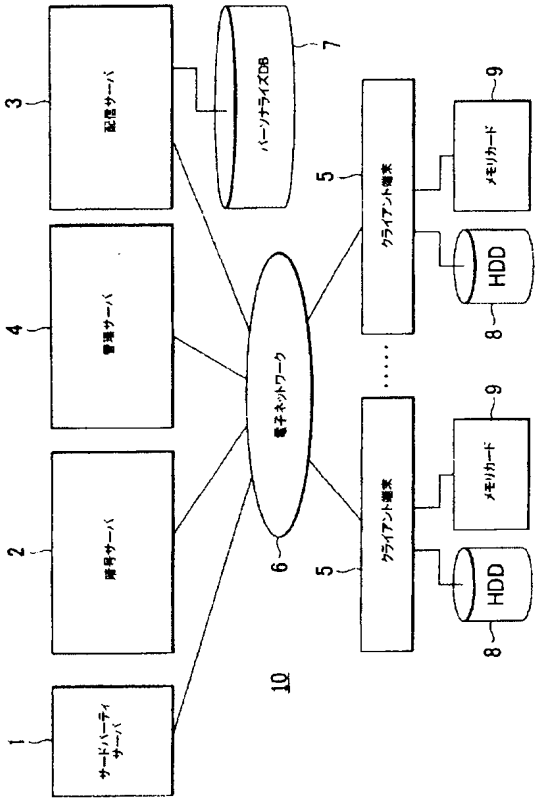
【００７６】

本発明によれば、電子レンタルチケットは、電子決済チケットで提供されるレンタル権と同様の又はそれ以上のレベルのレンタル権をユーザ（又はクライアント端末装置５）に好適に提供する。例えば、電子レンタルチケットは（電子決済チケットに復号化鍵が含まれていない場合）、コンピュータプログラムタイトル、レンタル期間、送金代価を特定し、及び暗号化されたコンピュータプログラムを復号化することが可能である復号化鍵のような付加情報を含む。電子レンタルチケットが復号化鍵を含むことは必須ではなく、実際このように復号化鍵が含まれる例は、単に例示的なものにすぎない。また、電子レンタルチケットは、復号化鍵を暗号化された形態で含むようにしてもよい。例えば、この暗号化を、機器ＩＤを使用して又は電子会員証明書（仮想ＩＤ等）の一部である他の情報を使用して行ってもよい。いずれにせよ、処理のこの時点ではユーザは所定レベルのレンタル権を受信するが、コンピュータプログラム又はコンピュータプログラムの暗号化されたバージョンをまだ受信してはいない。

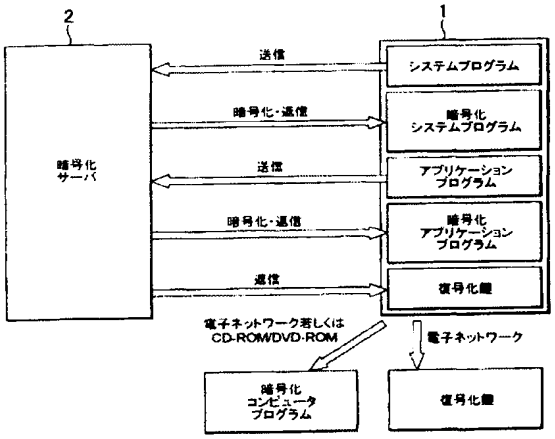
【００７７】
図２２に示されるように、クライアント端末５は、好適には、ネットワーク６を通じて配信装置と通信リンクを構築する（ステップＳ１０８）。これに応答して、配信装置では、上記のように例えば機器ＩＤ又は電子会員証明書を分析することで、クライアント端末５を識別する（ステップＳ１１０）。次に、クライアント端末５は、ネットワーク６を通じて配信装置に電子決済チケット（又は電子決済チケットの少なくとも一部）を伝送する（ステップＳ１１２）。好適には、これは配信装置に対して、クライアント端末５がレンタルに関するすべての必要な前ステップを完了し、コンピュータプログラムの暗号化されたバージョンを受信することが認可されたことを示す（ステップＳ１１４）。処理のこの時点でクライアント端末５は機器ＩＤ、電子会員証明書（存在する場合には仮想ＩＤも含む）、電子決済チケット、電子レンタルチケット、暗号化された復号化鍵及び暗号化コンピュータプログラムを好適に有する。
【００７８】
本発明によれば、ユーザは本発明の実施例に関連して上記処理を使用して、コンピュータプログラムをロード、インストール及び実行することが考えられる。本発明のレンタルシステムの実施例は、ネットワーク６を通じて、クライアント端末５の台数にかかわらずレンタルプログラムの安全な配信が可能となるという点で有利である。
【００７９】
以上、本発明を特定の実施形態により説明したが、実施形態は本発明の原理及び応用を単に例示的に説明したに過ぎない。従って、請求項に規定した本発明の精神及び範囲から逸脱することなく、これらの例示的な実施形態にたいして種々の変形をおこなうことができる。
【図面の簡単な説明】
【００８０】
【図１】本発明の１つ以上の形態に係る１人以上のユーザに対してのプログラムコンテンツ配布システムの模式図である。
【図２】図１に示すシステムの一部において実行される処理ステップを示す概念的ブロックとそのフローの説明図。
【図３】図１に示すシステムの一部において実行される処理ステップを示す概念的ブロックとそのフローの説明図。
【図４】図３に示された本発明に従って実行される処理ステップを示すフローチャート。
【図５】例えば、図１に示す管理サーバとクライアント端末により実行される処理ステップを示す概念的ブロック図とフローチャート。
【図６】図５に示す装置により実行されるさらなる処理ステップを示すフローチャート。
【図７】図１に示すシステムにより実行される処理ステップを示す概念的ブロック図。
【図８】図１に示すシステムにより実行される所定の処理ステップを示す概念的ブロック図とフローチャート。
【図９】図８に示す装置により実行されるさらなる処理ステップを示すフローチャート。
【図１０】本発明に係る所定のデータベースの内容を示す模式図。
【図１１】例えば、図１に示すクライアント端末により実行される、１つ以上の更なる処理手段を示すさらなる概念的ブロック図とフロー説明図。
【図１２】図１により実行される更なる処理ステップを示すフローチャート。
【図１３】本発明に係るクライアント端末により実行される１つ以上のさらなる処理ステップを示す概念的ブロック図とフロー説明図。
【図１４】図１３に示すさらなる詳細を鑑みた処理ステップを示すフローチャート。
【図１５】本発明のさらなる様態を示す概念的ブロック図とフローチャート。
【図１６】本発明の１つ以上の様態に従った所定のデータベースの内容を示す模式図。
【図１７】図１６に示すデータベースの内容の更なる機能を示す模式図。
【図１８】図１５に示すベース内容の更なる詳細を鑑みた処理ステップを示すフローチャート。

【図１９】本発明の１つ以上の形態を示すフローチャート。
【図２０】図１９に係る本発明の更なる処理ステップを示すフローチャート。
【図２１】図２０に係る本発明の更なる処理ステップを示すフローチャート。
【図２２】図２１に係る本発明の更なる処理ステップを示すフローチャート。

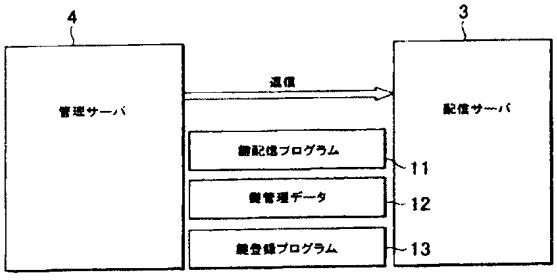
【図１】



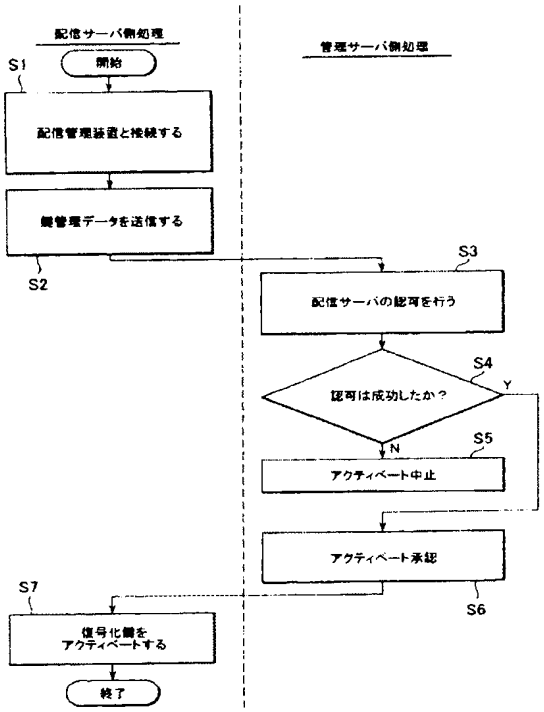
【図２】



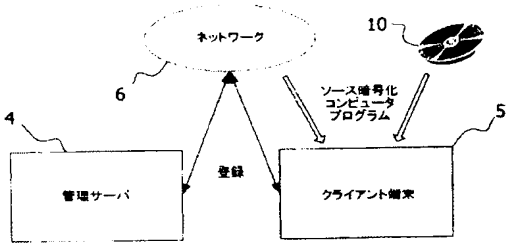
【図３】



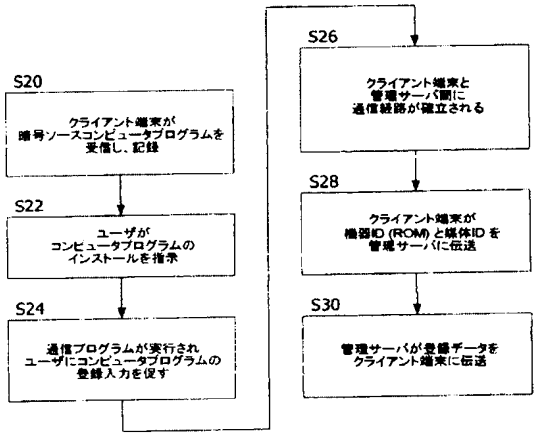
【図４】



【図５】



【図６】

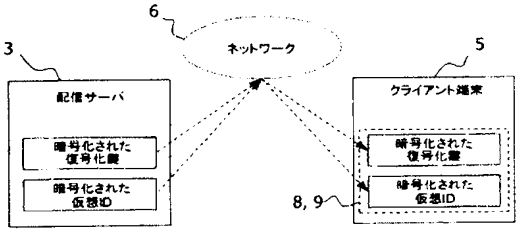


【図７】

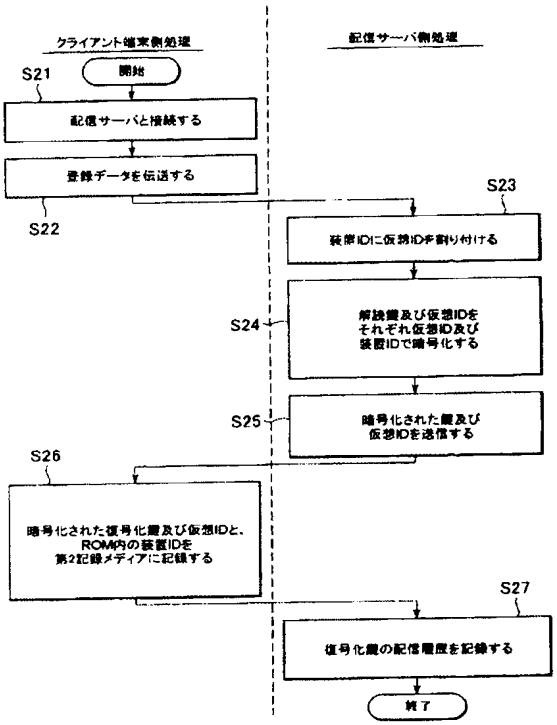
7A

デバイスID	配信元ID
K1234	D3456
K2345	D1278
K6789	--
K0987	--

【図８】



【図９】

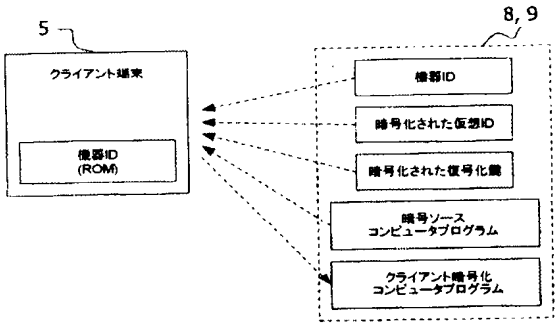


【図１０】

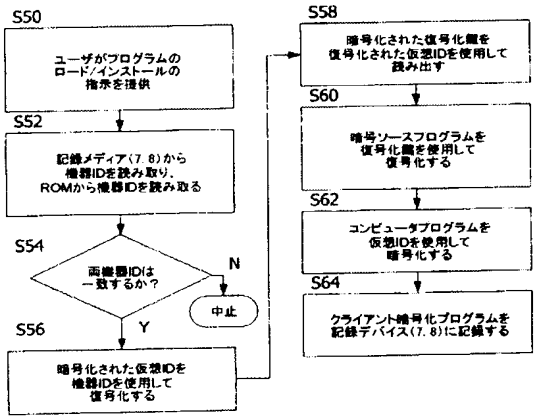
7

機器ID	仮想ID
K1234	———
K2345	B5678
K6789	B9012
K0987	———
⋮	⋮

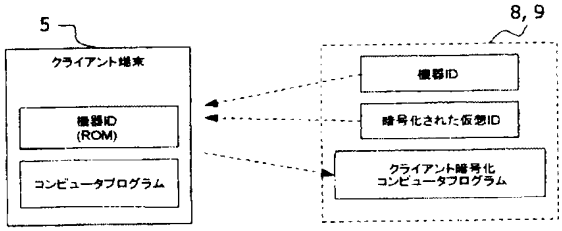
【図１１】



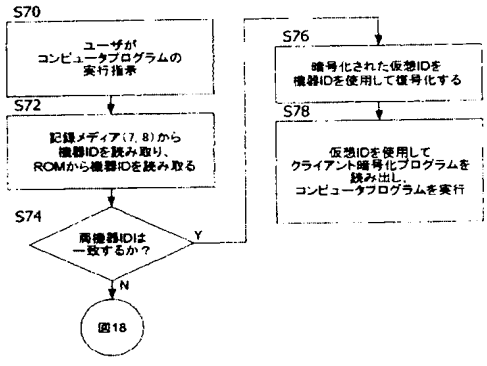
【図１２】



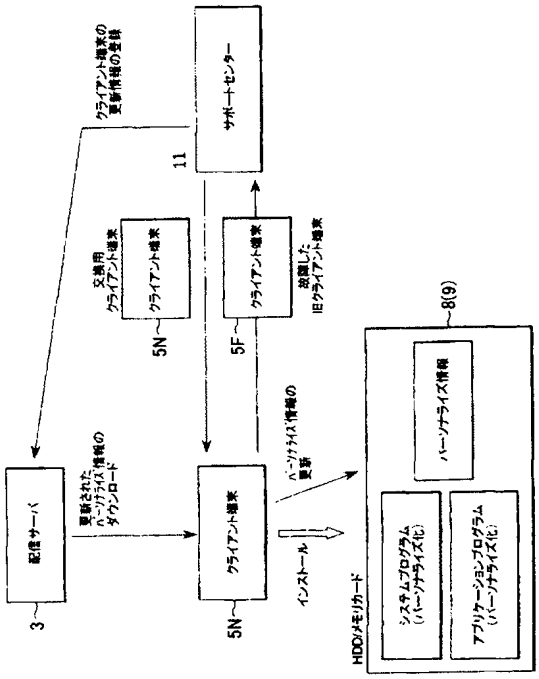
【図１３】



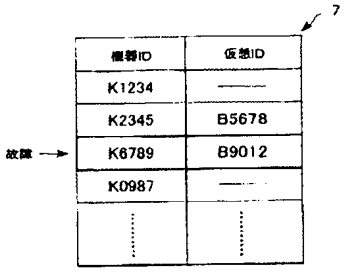
【図１４】



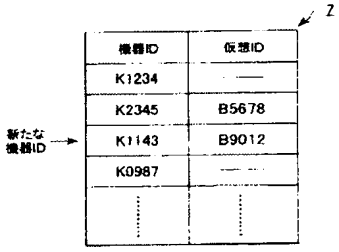
【図１５】



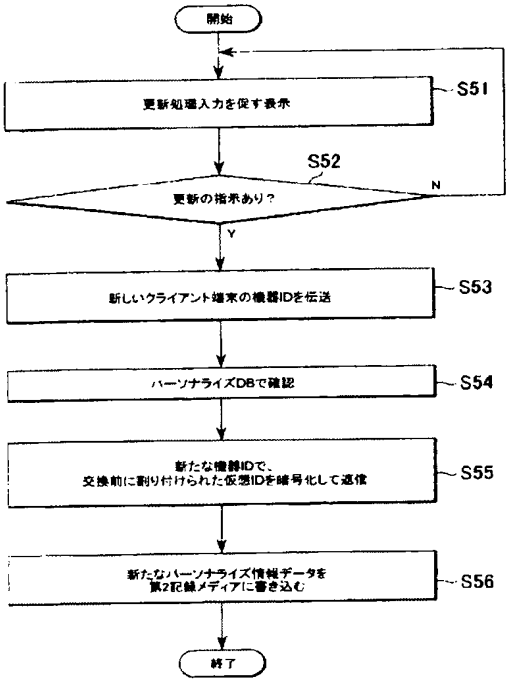
【図１６】



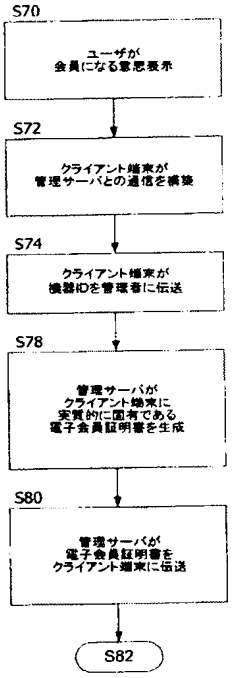
【図１７】



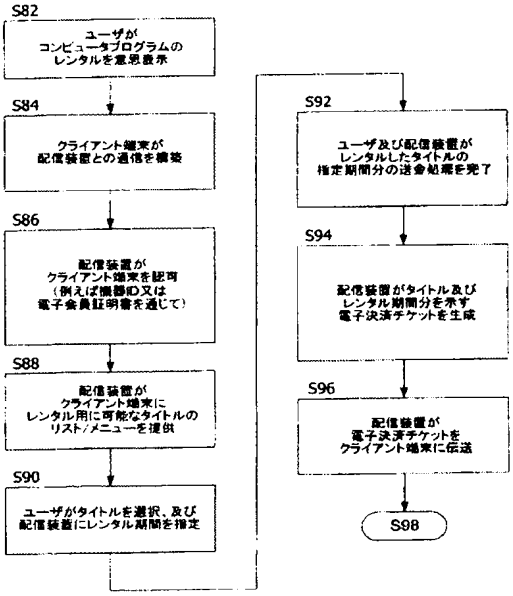
【図１８】



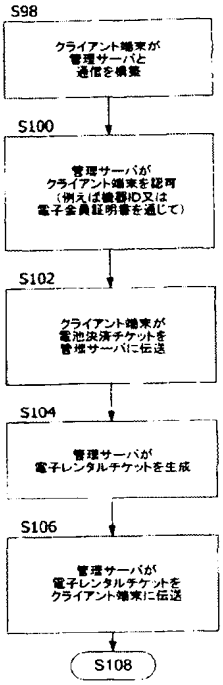
【図１９】



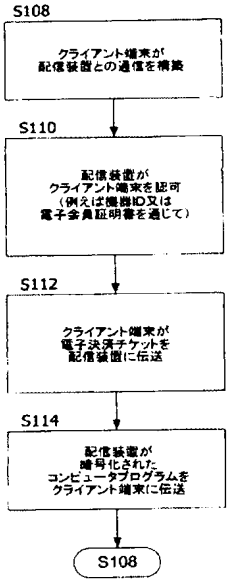
【図２０】



【図２１】


S98
クライアント端末が
管理サーバと
通信を構築
S100
管理サーバが
クライアント端末を認可
（例えば機器ID又は
電子会員証明書を通じて）
S102
クライアント端末が
電池決済チケットを
管理サーバに伝送
S104
管理サーバが
電子レンタルチケットを生成
S106
管理サーバが
電子レンタルチケットを
クライアント端末に伝送
S108

【図２２】


S108
クライアント端末が
配信装置との通信を構築
S110
配信装置が
クライアント端末を認可
（例えば機器ID又は
電子会員証明書を通じて）
S112
クライアント端末が
電子決済チケットを
配信装置に伝送
S114
配信装置が
暗号化された
コンピュータプログラムを
クライアント端末に伝送
S108

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/12738

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L 9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L 9/08, G06F 9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Japanese Utility Model Gazette 1926-1996, Japanese Publication of Unexamined Utility Model Applications 1971-2003, Japanese Registered Utility Model Gazette 1994-2003, Japanese Gazette Containing the Utility Model 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-242604 A (FUJITSU K.K.) 2000.09.08 page 4, column 5, line 46 -page 5, column 8, line 1 figures 1-2 (No families)	1-38
A	JP 11-275516 A (HITACHI SEISAKUSHYO K.K.) 1999.09.08 page 8, column 13, line 30 -page 8, column 14, line 5 figure 6 (No families)	1-38

☑ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14.03.03	25.03.03

Name and mailing address of the ISA/JP	Authorized officer	
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Hiromasa Nakazato (Seal) Telephone No. +81-3-3581-1101 Ext. 3599	5M 9364

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/12738

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/56068 A1 (THOMSON LICENSING S.A.) 2000.09.21 See whole document & AU 200036291 A & CN 1343420 A & EP 1169856 A1 & JP 2002-539724 A & KR 2001105384 A & MX 2001009286 A	1-38

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

フロントページの続き

(72)発明者　岡田　豊史
日本国東京都港区南青山２－６－２１　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　木本　陽介
日本国東京都港区南青山２－６－２１　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　金江　和広
日本国東京都港区南青山２－６－２１　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　小巻　賢二郎
日本国東京都港区南青山２－６－２１　株式会社ソニー・コンピュータエンタテインメント内
Ｆターム(参考) 5J104 EA17　EA18　EA26　PA07